On the genericity of maximum rank distance and Gabidulin codes

Neri, Alessandro ; Horlemann-Trautmann, Anna-Lena ; Randrianarisoa, Tovohery ; Rosenthal, Joachim

Abstract: We consider linear rank-metric codes in Fnqm. We show that the properties of being maximum rank distance (MRD) and non-Gabidulin are generic over the algebraic closure of the underlying field, which implies that over a large extension field a randomly chosen generator matrix generates an MRD and a non-Gabidulin code with high probability. Moreover, we give upper bounds on the respective probabilities in dependence on the extension degree m.

DOI: https://doi.org/10.1007/s10623-017-0354-4

On the Genericity of Maximum Rank Distance and Gabidulin Codes*

Alessandro Neri[2], Anna-Lena Horlemann-Trautmann[1], Tovohery Randrianarisoa[2] and Joachim Rosenthal[2]

[1]EPF Lausanne, Switzerland
[2]University of Zurich, Switzerland

May 20, 2016

Abstract

We consider linear rank-metric codes in $\mathbb{F}_{q^m}^n$. We show that the properties of being MRD (maximum rank distance) and non-Gabidulin are generic over the algebraic closure of the underlying field, which implies that over a large extension field a randomly chosen generator matrix generates an MRD and a non-Gabidulin code with high probability. Moreover, we give upper bounds on the respective probabilities in dependence on the extension degree m.

1 Introduction

Codes in the rank-metric have been studied for the last four decades. For linear codes a Singleton-type bound can be derived for these codes. In analogy to MDS codes in the Hamming metric, we call rank-metric codes that achieve the Singleton-type bound MRD (maximum rank distance) codes. Since the works of Delsarte [4] and Gabidulin [5] we know that linear MRD codes exist for any set of parameters. The codes they describe are called Gabidulin codes.

The question, if there are other general constructions of MRD codes that are not equivalent to Gabidulin codes, has been of large interest recently. Some constructions of non-Gabidulin MRD codes can be found e.g. in [2, 3, 11], where many of the derived codes are not linear over the underlying field but only linear over some subfield of it. For some small parameter sets, constructions of linear non-Gabidulin MRD codes were presented in [6]. On the other hand, in the same paper it was shown that all MRD codes in $\mathbb{F}_{2^4}^4$ are Gabidulin codes. In general, it remains an open question for which parameters non-Gabidulin MRD codes exist, and if so, how many such codes there are.

*This work was supported by SNF grant no. 149716.

In this paper we show that the properties of being MRD (maximum rank distance) and non-Gabidulin are generic. This implies that over a large field extension degree a randomly chosen generator matrix generates an MRD and a non-Gabidulin code with high probability. Moreover, we give an upper bound on the respective probabilities in dependence on the extension degree.

The paper is structured as follows. In Section 2 we give some preliminary definitions and results, first for rank-metric codes and then for the notion of genericity. Section 3 contains topological results, showing that the properties of being MRD and non-Gabidulin are generic. In Section 4 we derive some upper bounds on the probability of these two code properties in dependence on the extension degree of the underlying finite field. We conclude in Section 5.

2 Preliminaries

2.1 Finite Fields and Their Vector Spaces

The following definitions and results can be found in any textbook on finite fields, e.g. [8]. We denote the finite field of cardinality q by $\mathbb{F}_q$. It exists if and only if q is a prime power. Moreover, if it exists, $\mathbb{F}_q$ is unique up to isomorphism. An extension field of extension degree m is denoted by $\mathbb{F}_{q^m}$. If α is a root of an irreducible monic polynomial in $\mathbb{F}_q[x]$ of degree m, then

$$\mathbb{F}_{q^m} \cong \mathbb{F}_q[\alpha].$$

We now recall some basic theory on the trace function over finite fields.

Definition 2.1. Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^m}$ be an extension field. For $\alpha \in \mathbb{F}_{q^m}$, the *trace* of α over $\mathbb{F}_q$ is defined by

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) := \sum_{i=0}^{m-1} \alpha^{q^i}.$$

For every integer $0 < s < m$ with $\gcd(m, s) = 1$, we denote by φ_s the map given by

$$\begin{array}{rccc} \varphi_s : \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ \alpha & \longmapsto & \alpha^{q^s} - \alpha. \end{array}$$

The following result relates the trace with the maps φ_s.

Lemma 2.2. *The trace function satisfies the following properties:*

1. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$ *for all* $\alpha \in \mathbb{F}_{q^m}$.
2. $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *is a linear surjective transformation from* $\mathbb{F}_{q^m}$ *to* $\mathbb{F}_q$, *where* $\mathbb{F}_{q^m}$ *and* $\mathbb{F}_q$ *are considered as* $\mathbb{F}_q$*-vector spaces.*

3. *For every $\alpha \in \mathbb{F}_{q^m}^*$, the map T_α defined by*

$$\beta \longmapsto \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha\beta)$$

is a linear surjective transformation from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, where $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$ are considered as $\mathbb{F}_q$-vector spaces.

4. *φ_s is a linear transformation from $\mathbb{F}_{q^m}$ to itself, considered as $\mathbb{F}_q$-vector space.*

5. *For every s coprime to m, $\varphi_s(\alpha) = 0$ if and only if $\alpha \in \mathbb{F}_q$.*

6. $\ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}) = \mathrm{Im}(\varphi_s)$ *for every s coprime to m and has cardinality q^{m-1}.*

Proof. The statements of 1., 2. and 3. can be found e.g. in [8, Theorems 2.23 and 2.24].

4. For $\alpha, \beta \in \mathbb{F}_{q^m}$, $\varphi_s(\alpha+\beta) = (\alpha+\beta)^{q^s} - (\alpha+\beta) = \alpha^{q^s} - \alpha + \beta^{q^s} - \beta = \varphi_s(\alpha) + \varphi_s(\beta)$. Moreover, for every $\alpha \in \mathbb{F}_{q^m}$, $c \in \mathbb{F}_q$, $\varphi_s(\alpha) = c^{q^s}\alpha^{q^s} - c\alpha = c\left(\alpha^{q^s} - \alpha\right) = c\varphi_s(\alpha)$.

5. We have $\varphi_s(\alpha) = \alpha^{q^s} - \alpha = 0$ if and only if $\alpha \in \mathbb{F}_{q^s}$. Since $\alpha \in \mathbb{F}_{q^m}$, this is true if and only if $\alpha \in \mathbb{F}_{q^m} \cap \mathbb{F}_{q^s} = \mathbb{F}_q$.

6. First we show that $\mathrm{Im}(\varphi_s) \subseteq \ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})$. Consider an element $\alpha \in \mathrm{Im}(\varphi_s)$. Then there exists $\beta \in \mathbb{F}_{q^m}$ such that $\alpha = \beta^{q^s} - \beta$. Now

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta^{q^s} - \beta) = \sum_{i=0}^{m-1} (\beta^{q^s} - \beta)^{q^i} = \sum_{i=0}^{m-1} \beta^{q^{s+i}} - \sum_{i=0}^{m-1} \beta^{q^i}.$$

We observe now that if $i \equiv j \mod m$, then $\beta^{q^i} = \beta^{q^j}$. Hence the sum $\sum_{i=0}^{m-1} \beta^{q^{s+i}}$ is a rearrangement of $\sum_{i=0}^{m-1} \beta^{q^i}$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0$. At this point observe that the trace function is a polynomial of degree q^{m-1} and so it has at most q^{m-1} roots. This means that $|\ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})| \leq q^{m-1}$. By part 4 and 5 of this Lemma

$$|\mathrm{Im}(\varphi_s)| = \frac{|\mathbb{F}_{q^m}|}{|\ker(\varphi_s)|} = q^{m-1}$$

and therefore $\mathrm{Im}(\varphi_s)$ and $\ker(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})$ must be equal.

□

We denote by $\mathrm{GL}_n(q) := \{A \in \mathbb{F}_q^{n\times n} \mid \mathrm{rk}(A) = n\}$ the general linear group of degree n over $\mathbb{F}_q$. Furthermore we need the Gaussian binomial $\binom{n}{k}_q$, which is defined as the number of k-dimensional vector spaces of $\mathbb{F}_q^n$. It is well-known that

$$\binom{n}{k}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i} = \frac{\prod_{i=0}^{k-1}(q^n - q^i)}{|\mathrm{GL}_k(q)|}.$$

Moreover, the following fact is well-known and easy to see.

Lemma 2.3. *Let k, n be two integers such that $0 < k \leq n$, and let $\mathcal{U}$ be a k-dimensional vector subspace of $\mathbb{F}_q^n$. Then, for every $r = 0, \ldots, k$, the number of k-dimensional subspaces that intersect $\mathcal{U}$ in a $(k-r)$-dimensional subspace is*

$$\begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}.$$

Proof. There are $\begin{bmatrix} k \\ k-r \end{bmatrix}_q$ many subspaces $\mathcal{U}'$ of $\mathcal{U}$ of dimension $(k-r)$ that can be the intersection space. Now, in order to complete $\mathcal{U}'$ to a k-dimensional vector space, intersecting $\mathcal{U}$ only in $\mathcal{U}'$, we have $\prod_{i=0}^{r-1}(q^n - q^{k+i})$ choices for the remaining basis vectors. For counting how many of these bases span the same space we just need to count the number of $k \times k$ matrices of the form

$$\begin{bmatrix} I_{k-r} & 0 \\ A & B \end{bmatrix},$$

where $A \in \mathbb{F}_q^{r \times (k-r)}$ and $B \in \mathrm{GL}_r(q)$. Hence the final count is given by

$$\begin{aligned} \begin{bmatrix} k \\ k-r \end{bmatrix}_q \frac{\prod_{i=0}^{r-1}(q^n - q^{k+i})}{q^{r(k-r)}|\mathrm{GL}_r(q)|} &= \begin{bmatrix} k \\ k-r \end{bmatrix}_q \frac{q^{kr}\prod_{i=0}^{r-1}(q^{n-k} - q^i)}{q^{r(k-r)}|\mathrm{GL}_r(q)|} \\ &= \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}. \end{aligned}$$

□

2.2 Rank-metric Codes

Recall that there always exists $\alpha \in \mathbb{F}_{q^m}$, such that $\mathbb{F}_{q^m} \cong \mathbb{F}_q[\alpha]$. Moreover, $\mathbb{F}_{q^m}$ is isomorphic (as a vector space over $\mathbb{F}_q$) to the vector space $\mathbb{F}_q^m$. One then easily obtains the isomorphic description of matrices over the base field $\mathbb{F}_q$ as vectors over the extension field, i.e. $\mathbb{F}_q^{m \times n} \cong \mathbb{F}_{q^m}^n$.

Definition 2.4. The *rank distance* d_R on $\mathbb{F}_q^{m \times n}$ is defined by

$$d_R(X, Y) := \mathrm{rk}(X - Y), \quad X, Y \in \mathbb{F}_q^{m \times n}.$$

Analogously, we define the rank distance between two elements $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ as the rank of the difference of the respective matrix representations in $\mathbb{F}_q^{m \times n}$.

In this paper we will focus on $\mathbb{F}_{q^m}$-linear rank-metric codes in $\mathbb{F}_{q^m}^n$, i.e. those codes that form a vector space over $\mathbb{F}_{q^m}$.

Definition 2.5. An *$\mathbb{F}_{q^m}$-linear rank-metric code* $\mathcal{C}$ of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_{q^m}^n$ equipped with the rank distance. A matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ is called a *generator matrix* for the code $\mathcal{C}$ if

$$\mathcal{C} = \mathrm{rs}(G),$$

where $\mathrm{rs}(G)$ is the subspace generated by the rows of the matrix G, called the *row space* of G.

Whenever we talk about linear codes in this work, we will mean linearity over the extension field $\mathbb{F}_{q^m}$. The well-known Singleton bound for codes in the Hamming metric implies also an upper bound for codes in the rank-metric:

Theorem 2.6. *[5, Section 2] Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear matrix code with minimum rank distance d of dimension k. Then*

$$k \leq n - d + 1.$$

Definition 2.7. A code attaining the Singleton bound is called a *maximum rank distance (MRD) code.*

Lemma 2.8. *[6, Lemma 5.3] Any linear MRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k has a generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ in systematic form, i.e.*

$$G = \left[\; I_k \; \middle| \; X \; \right]$$

Moreover, all entries in X are from $\mathbb{F}_{q^m} \backslash \mathbb{F}_q$.

For some vector $(v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ we denote the $k \times n$ *s-Moore matrix* by

$$M_{s,k}(v_1, \ldots, v_n) := \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1^{[s]} & v_2^{[s]} & \ldots & v_n^{[s]} \\ \vdots & & & \vdots \\ v_1^{[s(k-1)]} & v_2^{[s(k-1)]} & \ldots & v_n^{[s(k-1)]} \end{pmatrix},$$

where $[i] := q^i$.

Definition 2.9. Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$ and let s be coprime to m. We define a *generalized Gabidulin code* $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k as the linear block code with generator matrix $M_{s,k}(g_1, \ldots, g_n)$. Using the isomorphic matrix representation we can interpret $\mathcal{C}$ as a matrix code in $\mathbb{F}_q^{m \times n}$.

Note that for $s = 1$ the previous definition coincides with the classical Gabidulin code construction. The following theorem was shown for $s = 1$ in [5, Section 4], and for general s in [7].

Theorem 2.10. *A generalized Gabidulin code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k over $\mathbb{F}_{q^m}$ has minimum rank distance $n - k + 1$. Thus generalized Gabidulin codes are MRD codes.*

The dual code of a code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is defined in the usual way as

$$\mathcal{C}^\perp := \{\boldsymbol{u} \in \mathbb{F}_{q^m}^n \mid \boldsymbol{u}\boldsymbol{c}^T = 0 \quad \forall \boldsymbol{c} \in \mathcal{C}\}.$$

In his seminal paper Gabidulin showed the following two results on dual codes of MRD and Gabidulin codes. The result was generalized to $s > 1$ later on by Kshevetskiy and Gabidulin.

Proposition 2.11. *[5, Sections 2 and 4][7, Subsection IV.C]*

1. *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code of dimension k. Then the dual code $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^m}^n$ is an MRD code of dimension $n-k$.*

2. *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a generalized Gabidulin code of dimension k. Then the dual code $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^m}^n$ is a generalized Gabidulin code of dimension $n-k$.*

For more information on bounds and constructions of rank-metric codes the interested reader is referred to [5].

Denote by $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ the *Galois group* of $\mathbb{F}_{q^m}$, consisting of the automorphisms of $\mathbb{F}_{q^m}$ that fix the base field $\mathbb{F}_q$ (i.e., for $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $\alpha \in \mathbb{F}_q$ we have $\sigma(\alpha) = \alpha$). It is well-known that $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is generated by the *Frobenius map*, which takes an element to its q-th power. Hence the automorphisms are of the form $x \mapsto x^{[i]}$ for some $0 \leq i \leq m$.

Given a matrix (resp. a vector) $A \in \mathbb{F}_{q^m}^{k \times n}$, we denote by $A^{([s])}$ the component-wise Frobenius A, i.e., every entry of the matrix (resp. the vector) is raised to its q^s-th power. Analogously, given some $\mathcal{C} \subseteq \mathbb{F}_{q^m}^{k \times n}$, we define

$$\mathcal{C}^{([s])} := \left\{ \mathbf{c}^{([s])} \mid \mathbf{c} \in \mathcal{C} \right\}.$$

The (semi-)linear rank isometries on $\mathbb{F}_{q^m}^n$ are induced by the isometries on $\mathbb{F}_q^{m \times n}$ and are hence well-known, see e.g. [1, 9, 12]:

Lemma 2.12. *[9, Proposition 2] The semilinear $\mathbb{F}_q$-rank isometries on $\mathbb{F}_{q^m}^n$ are of the form*

$$(\lambda, A, \sigma) \in \left(\mathbb{F}_{q^m}^* \times \mathrm{GL}_n(q)\right) \rtimes \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q),$$

acting on $\mathbb{F}_{q^m}^n \ni (v_1, \ldots, v_n)$ via

$$(v_1, \ldots, v_n)(\lambda, A, \sigma) = (\sigma(\lambda v_1), \ldots, \sigma(\lambda v_n))A.$$

In particular, if $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is a linear code with minimum rank distance d, then

$$\mathcal{C}' = \sigma(\lambda \mathcal{C})A$$

is a linear code with minimum rank distance d.

One can easily check that $\mathbb{F}_q$-linearly independent elements in $\mathbb{F}_{q^m}$ remain $\mathbb{F}_q$-linearly independent under the actions of $\mathbb{F}_{q^m}^*, \mathrm{GL}_n(q)$ and $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Moreover, the s-Moore matrix structure is preserved under these actions, which implies that the class of generalized Gabidulin codes is closed under the semilinear isometries. Thus a code is semilinearly isometric to a generalized Gabidulin code if and only if it is itself a generalized Gabidulin code.

In this work we need the following criteria for both the MRD and the Gabidulin property. The following criterion for MRD codes was given in [6], which in turn is based on a well-known result given in [5]:

Proposition 2.13. *Let $G \in \mathbb{F}_{q^m}^{k\times n}$ be a generator matrix of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Then $\mathcal{C}$ is an MRD code if and only if*

$$\mathrm{rk}(VG^T) = k$$

for all $V \in \mathbb{F}_q^{k\times n}$ with $\mathrm{rk}(V) = k$.

Furthermore, we need the following criterion for the generalized Gabidulin property:

Theorem 2.14. *[6, Theorem 4.8] Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code of dimension k. $\mathcal{C}$ is a generalized Gabidulin code if and only if there exists s with $\gcd(s, m) = 1$ such that*

$$\dim(\mathcal{C} \cap \mathcal{C}^{([s])}) = k - 1.$$

2.3 The Zariski Topology over Finite Fields

Consider the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_r]$ over the base field $\mathbb{F}_q$ and denote by $\bar{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$, necessarily an infinite field. For a subset $S \subseteq \mathbb{F}_q[x_1, \ldots, x_r]$ one defines the algebraic set

$$V(S) := \{\boldsymbol{x} \in \bar{\mathbb{F}}_q^r \mid f(\boldsymbol{x}) = 0, \forall f \in S\}.$$

It is well-known that the algebraic sets inside $\bar{\mathbb{F}}_q^r$ form the *closed sets* of a topology, called the *Zariski topology*. The complements of the Zariski-closed sets are the *Zariski-open* sets.

Definition 2.15. One says that a subset $G \subset \bar{\mathbb{F}}_q^r$ defines a *generic set* if G contains a non-empty Zariski-open set.

If the base field are the real number ($\mathbb{R}$) or complex numbers ($\mathbb{C}$), then a generic set inside $\mathbb{R}^r$ (respectively inside $\mathbb{C}^r$) is necessarily dense and its complement is contained in an algebraic set of dimension at most $r - 1$.

Over a finite field $\mathbb{F}_q$ one has to be a little bit more careful. Indeed for every subset $T \subset \mathbb{F}_q^r$ one finds a set of polynomials $S \subseteq \mathbb{F}_q[x_1, \ldots, x_r]$ such that

$$\{\boldsymbol{x} \in \mathbb{F}_q^r \mid f(\boldsymbol{x}) = 0, \forall f \in S\} = T.$$

This follows simply from the fact that a single point inside $\mathbb{F}_q^r$ forms a Zariski-closed set and any subset $T \subset \mathbb{F}_q^r$ is a finite union of points. However if one has an algebraic set $V(S)$, as defined in the beginning of this subsection, then the $\mathbb{F}_{q^m}$-rational points defined through

$$V(S; \mathbb{F}_{q^m}) := \{\boldsymbol{x} \in \mathbb{F}_{q^m}^r \mid f(\boldsymbol{x}) = 0, \forall f \in S\}$$

become in proportion to the whole vector space $\mathbb{F}_{q^m}^r$ thinner and thinner, as the extension degree m increases. This is a consequence of the Schwartz-Zippel Lemma which we will formulate, for our purposes, over a finite field. The lemma itself will be crucial for our probability estimations in Section 4.

Lemma 2.16 (Schwartz-Zippel)**.** *[10, Corollary 1] Let $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_r]$ be a non-zero polynomial of total degree $d \geq 0$. Let $\mathbb{F}_{q^n}$ be an extension field and let $S \subseteq \mathbb{F}_{q^n}$ be a finite set. Let $v_1, v_2, \ldots, v_r$ be selected at random independently and uniformly from S. Then*

$$\Pr\big(f(v_1, v_2, \ldots, v_r) = 0\big) \leq \frac{d}{|S|}.$$

3 Topological Results

The idea of this section is to show that the properties of being MRD and non-Gabidulin are generic properties.

Recall that, by Lemma 2.8, every linear MRD code in $\mathbb{F}_{q^m}^n$ of dimension k has a unique representation by its generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ in systematic form

$$G = [\, I_k \mid X \,].$$

Thus we have a one-to-one correspondence between the set of linear MRD codes in $\mathbb{F}_{q^m}^n$ and a subset of the set of matrices $\mathbb{F}_{q^m}^{k \times (n-k)}$. Therefore we want to investigate how many matrices $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$ give rise to an MRD or a generalized Gabidulin code, when plugged into the above form of a systematic generator matrix.

However, to make sense of the definition of genericity, we need to do this investigation over the algebraic closure of $\mathbb{F}_{q^m}$. Unfortunately though, some results in the rank-metric, in particular the definition of and results related to generalized Gabidulin codes, do not hold over infinite fields. Therefore we will actually show that the set of matrices fulfilling the criteria of Corollary 2.13 (for being MRD) and Theorem 2.14 (for being a generalized Gabidulin code) are generic sets over the algebraic closure.

We first show that the set of generator matrices fulfilling the MRD criterion of Corollary 2.13 is generic.

Theorem 3.1. *Let $1 \leq k \leq n-1$. The set*

$$S_{\text{MRD}} := \{X \in \bar{\mathbb{F}}_{q^m}^{k \times (n-k)} \mid \forall A \in \mathbb{F}_q^{n \times k} \text{ of rank } k : \det([I_k \mid X]A) \neq 0\}$$

is a generic subset of $\bar{\mathbb{F}}_{q^m}^{k \times (n-k)}$.

Proof. We need to show that S_{MRD} contains a non-empty Zariski-open set. In fact we will show that S_{MRD} is a non-empty Zariski-open set. The non-empty-ness follows from the existence of Gabidulin codes for every set of parameters. Hence it remains to show that it is Zariski-open.

If we denote the entries of $X \in \bar{\mathbb{F}}_{q^m}^{k(n-k)}$ as the variables $x_1, \ldots, x_{k(n-k)}$, then, for a

given $A \in \mathbb{F}_q^{n\times k}$, we have $\det([I_k \mid X]A) \in \mathbb{F}_q[x_1, \ldots, x_{k(n-k)}]$. Hence we can write

$$\begin{aligned} S_{\mathrm{MRD}} &= \bigcap_{\substack{A\in\mathbb{F}_q^{n\times k}\\ \mathrm{rk}(A)=k}} \{X \in \bar{\mathbb{F}}_{q^m}^{k\times(n-k)} \mid \det([I_k \mid X]A) \neq 0\} \\ &= \bigcap_{\substack{A\in\mathbb{F}_q^{n\times k}\\ \mathrm{rk}(A)=k}} V(\det([I_k \mid X]A))^C, \end{aligned}$$

i.e., it is a finite intersection of Zariski-open sets. Therefore S_{MRD} is a Zariski-open set. □

Remark 3.2. In Theorem 3.1 we chose the MRD criterion of Corollary 2.13 to show that the MRD property (if seen over some finite extension field) is generic. One can do the same by using the MRD criterion of Horlemann-Trautmann-Marshall from [6, Corollary 3].

We now turn to generalized Gabidulin codes. Firstly we rewrite the criterion from Theorem 2.14 in a more suitable way.

Lemma 3.3. *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code of dimension k and let $0 < s < m$ with $\gcd(s, m) = 1$. $\mathcal{C}$ is a generalized Gabidulin code with parameter s if and only if $\mathrm{rk}(X^{(q^s)} - X) = 1$.*

Proof. We know from Theorem 2.14 that an MRD code $\mathcal{C} = \mathrm{rs}[I_k \mid X] \subseteq \mathbb{F}_{q^m}^n$ is a generalized Gabidulin code if and only if $\dim(\mathcal{C} \cap \mathcal{C}^{(q^s)}) = k - 1$. We get

$$\begin{aligned} &\dim(\mathcal{C} \cap \mathcal{C}^{(q^s)}) = k - 1 \\ \iff &\mathrm{rk}\left[\begin{array}{c|c} I_k & X \\ I_k & X^{(q^s)} \end{array}\right] = k + 1 \\ \iff &\mathrm{rk}\left[\begin{array}{c|c} I_k & X \\ 0 & X^{(q^s)} - X \end{array}\right] = k + 1 \\ \iff &\mathrm{rk}(X^{(q^s)} - X) = 1. \end{aligned}$$

□

The following theorem shows that the set of generator matrices not fulfilling the generalized Gabidulin criterion of Lemma 3.3 is generic over the algebraic closure.

Theorem 3.4. *Let $1 \leq k \leq n - 1$ and $0 < s < m$ with $\gcd(s, m) = 1$. Moreover, let $S_{\mathrm{MRD}} \subseteq \bar{\mathbb{F}}_{q^m}^{k\times(n-k)}$ be as defined in Theorem 3.1. The set*

$$S_{\mathrm{Gab},s} := \{X \in \bar{\mathbb{F}}_{q^m}^{k\times(n-k)} \mid \mathrm{rk}(X^{(q^s)} - X) = 1\} \cap S_{\mathrm{MRD}}$$

is a Zariski-closed subset of the Zariski-open set S_{MRD}.

Proof. Let $X \in S_{\mathrm{Gab},s}$. Since $X \in S_{\mathrm{MRD}}$, it follows from Lemma 2.8 that $X_{ij} \notin \mathbb{F}_q$ for $i = 1, \ldots, k$ and $j = 1, \ldots, n-k$. Then the condition $\mathrm{rk}(X^{(q^s)} - X) = 1$ is equivalent to $\mathrm{rk}(X^{(q^s)} - X) < 2$, which in turn is equivalent to the condition that all 2×2-minors of $(X^{(q^s)} - X)$ are zero. If we denote the entries of $X \in \bar{\mathbb{F}}_{q^m}^{k(n-k)}$ as the variables $x_1, \ldots, x_{k(n-k)}$, then these 2×2-minors of $(X^{(q^s)} - X)$ are elements of $\mathbb{F}_q[x_1, \ldots, x_{k(n-k)}]$. Let us call the set of all these minors S'. Then

$$\begin{aligned} S_{\mathrm{Gab},s} &= \left\{ X \in \bar{\mathbb{F}}_{q^m}^{k \times (n-k)} \mid f(x_1, \ldots, x_{k(n-k)}) = 0, \forall f \in S' \right\} \cap S_{\mathrm{MRD}} \\ &= V(S') \cap S_{\mathrm{MRD}}. \end{aligned}$$

Hence it is a Zariski-closed subset of $S_{\mathrm{MRD}} \subseteq \bar{\mathbb{F}}_{q^m}^{k \times (n-k)}$. □

Theorem 3.4 implies that the complement of $S_{\mathrm{Gab},s}$, i.e., the set of matrices that fulfill the MRD criterion but do not fulfill the generalized Gabidulin criterion, is a Zariski-open subset of $S_{\mathrm{MRD}} \subset \bar{\mathbb{F}}_{q^m}^{k \times (n-k)}$. Thus, if it is non-empty, then the complement of $S_{\mathrm{Gab},s}$ is a generic set. The non-empty-ness of this set will be shown in the following section, in Theorem 4.12.

In other words, over the algebraic closure, a randomly chosen generator matrix gives rise to a code that does not fulfill the generalized Gabidulin criterion with high probability.

4 Probability Estimations

In the previous section we have used the Zariski topology to show that a randomly chosen linear code over $\bar{\mathbb{F}}_{q^m}$ fulfills most likely the MRD criterion but not the generalized Gabidulin criterion. Intuitively this tells us that over a finite, but large, extension field of $\mathbb{F}_q$ a randomly chosen linear code is most likely an MRD code but not a generalized Gabidulin code. In this section we derive some bounds on the probability that this statement is true, in dependence of the field extension degree m.

4.1 Probability for MRD codes

Here we give a lower bound on the probability that a random linear rank-metric code in $\mathbb{F}_{q^m}^n$ is MRD. A straight-forward approach gives the following result.

Theorem 4.1. *Let $X \in \mathbb{F}_{q^m}^{k(n-k)}$ be randomly chosen. Then*

$$\Pr\big(\mathrm{rs}[I_k \mid X] \text{ is an MRD code } \big) \geq 1 - \frac{k \prod_{i=0}^{k-1} (q^n - q^i)}{q^m} \geq 1 - k q^{kn-m}.$$

Proof. It follows from Corollary 2.13 that $\mathrm{rs}[I_k \mid X]$ is a non-MRD code if and only if

$$p^* := \prod_{\substack{A \in \mathbb{F}_q^{n \times k} \\ \mathrm{rk}(A) = k}} \det([I_k \mid X]A) = 0.$$

If we see the entries of X as the variables $x_1, \ldots, x_{k(n-k)}$, then every variable x_i is contained in at most one row of the matrix

$$[I_k \,|\, X]A = (\sum_{\ell=1}^{k} A_{\ell j} + \sum_{\ell=k+1}^{n} X_{i\ell} A_{\ell j})_{i,j}.$$

Thus $\det([I_k \mid X]A) \in \mathbb{F}_q[x_1, \ldots, x_{k(n-k)}]$ has degree at most k. The number of matrices in $\mathbb{F}_q^{n\times k}$ of rank k is $\prod_{i=0}^{k-1}(q^n - q^i) \leq q^{kn}$, hence the degree of p^* is at most $k\prod_{i=0}^{k-1}(q^n - q^i)$. It follows from Lemma 2.16 that

$$\Pr\big(\text{ rs}[I_k \mid X] \text{ is not an MRD code }\big) \leq \frac{\deg p^*}{q^m}$$

and hence

$$\Pr\big(\text{ rs}[I_k \mid X] \text{ is an MRD code }\big) \geq 1 - \frac{\deg p^*}{q^m} \geq 1 - \frac{k\prod_{i=0}^{k-1}(q^n - q^i)}{q^m} \geq 1 - kq^{kn-m}.$$

□

In the remainder of this subsection we want to improve the bound obtained in Theorem 4.1. To do so we introduce the set

$$\mathcal{T}(k,n) = \left\{E \in \mathbb{F}_q^{k\times n} \,|\, E \text{ is in reduced row echelon form and } \mathrm{rk}(E) = k\right\}.$$

With this notation we can formulate a variation of Corollary 2.13:

Proposition 4.2. *Let $G \in \mathbb{F}_{q^m}^{k\times n}$ be a generator matrix of a rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$. Then $\mathcal{C}$ is an MRD code if and only if*

$$\mathrm{rk}(EG^T) = k$$

for all $E \in \mathcal{T}(k,n)$.

Proof. For every matrix $V \in \mathbb{F}_q^{k\times n}$ consider its reduced row echelon form E_V. I.e., there exists a matrix $R \in \mathrm{GL}_k(q)$ such that $V = RE_V$. Then

$$\det(VG^T) = \det(RE_VG^T) = \det(R)\det(E_VG^T),$$

and since $\det(R) \neq 0$ we obtain that $\mathrm{rk}(VG^T) = k$ if and only if $\mathrm{rk}(E_VG^T) = k$. By Corollary 2.13 the statement follows. □

For $E \in \mathcal{T}(k,n)$ we define the polynomial

$$f_E(x_1, \ldots, x_{k(n-k)}) := \det([I_k \,|\, X]E^T) \in \mathbb{F}_{q^m}[x_1, \ldots, x_{k(n-k)}],$$

and we furthermore define

$$f^*(x_1, \ldots, x_{k(n-k)}) := \mathrm{lcm}\left\{f_E(x_1, \ldots, x_{k(n-k)}) \,|\, E \in \mathcal{T}(k,n)\right\},$$

where, as before, the entries of X are the variables $x_1, \ldots, x_{k(n-k)}$. We can easily observe the following.

Proposition 4.3. *The set of linear non-MRD codes of dimension k in $\mathbb{F}_{q^m}^n$ is in one-to-one correspondence with the algebraic set*

$$V(\{f^*\}) = \left\{(v_1, \ldots, v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid f^*(v_1, \ldots, v_{k(n-k)}) = 0\right\}.$$

Proof. It follows from Proposition 4.2 that the set of linear non-MRD codes of dimension k in $\mathbb{F}_{q^m}^n$ is in one-to-one correspondence with the algebraic set

$$\begin{aligned} V &= \bigcup_{E \in \mathcal{T}(k,n)} \left\{(v_1, \ldots, v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid f_E(v_1, \ldots, v_{k(n-k)}) = 0\right\} \\ &= \left\{(v_1, \ldots, v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid \prod_{E \in \mathcal{T}(k,n)} f_E(v_1, \ldots, v_{k(n-k)}) = 0\right\} \\ &= \left\{(v_1, \ldots, v_{k(n-k)}) \in \mathbb{F}_{q^m}^{k(n-k)} \mid f^*(v_1, \ldots, v_{k(n-k)}) = 0\right\}, \end{aligned}$$

where the last two equalities follow from the well-known fact that

$$V(\{f\}) \cup V(\{g\}) = V(\{fg\}) = V(\{\mathrm{lcm}(f, g)\})$$

for any $f, g \in \mathbb{F}_q[x_1, \ldots, x_{k(n-k)}]$. □

Note that in the definition of an algebraic set, it suffices to use the square-free part of the defining polynomial(s). In the above definition of V however, $f^*(x_1, \ldots, x_{k(n-k)})$ is already square-free, as we show in the following.

Lemma 4.4. *For every $E \in \mathcal{T}(k, n)$ the polynomial $f_E(x_1, \ldots, x_{k(n-k)})$ is square-free. In particular, the polynomial $f^*(x_1, \ldots, x_{k(n-k)})$ is square-free.*

Proof. As in the proof of Theorem 4.1, every variable x_i is contained in at most one row of the matrix $[I_k \mid X]E^T$. Hence, in the polynomial $f_E(x_1, \ldots, x_{k(n-k)})$ the degree with respect to every variable is at most 1. Thus $f_E(x_1, \ldots, x_{k(n-k)})$ cannot have multiple factors. □

We now determine an upper bound on the degree of the defining polynomial f^*.

Lemma 4.5. *Let $E \in \mathcal{T}(k, n)$ and let $\mathcal{U}_0$ be the subspace of $\mathbb{F}_q^n$ defined by*

$$\mathcal{U}_0 := \mathrm{rs}[\, I_k \mid 0 \,] = \left\{(u_1, \ldots, u_n) \in \mathbb{F}_q^n \mid u_{k+1} = u_{k+2} = \ldots = u_n = 0\right\}.$$

Then

$$\deg f_E = k - \dim\left(\mathrm{rs}(E) \cap \mathcal{U}_0\right).$$

Proof. Let $r := k - \dim\left(\mathrm{rs}(E) \cap \mathcal{U}_0\right)$ with $0 \leq r \leq k$. We can write

$$E^T = \left[\frac{E_1}{E_2}\right],$$

where $E_1 \in \mathbb{F}_q^{k\times k}, E_2 \in \mathbb{F}_q^{(n-k)\times k}$. Since $\dim(\mathrm{rs}(E) \cap \mathcal{U}_0) = k - r$, we have $\mathrm{rk}(E_2) = r$. Thus there exists a matrix $R \in \mathrm{GL}_k(q)$ such that the first r columns of E_2R are linearly independent and the last $k - r$ columns are zero. Then

$$f_E(x_1, \ldots, x_{k(n-k)}) = \det([\ I_k \mid X\ ]E^T) = \det(R)^{-1} \det(E_1R + XE_2R).$$

The last $k - r$ columns of the matrix XE_2R are zero, i.e., the last $k - r$ columns of $E_1R + XE_2R$ do not contain any of the variables x_i. On the other hand, the entries of the first r columns are polynomials in $\mathbb{F}_q[x_1, \ldots, x_{k(n-k)}]$ of degree 1, since

$$E_1R + XE_2R = \left(\sum_{\ell=1}^{n} (E_1)_{i\ell} R_{\ell j} + \sum_{\ell=1}^{k} \sum_{\ell'=1}^{n} X_{i\ell'} (E_2)_{\ell'\ell} R_{\ell j} \right)_{i,j}.$$

Hence we have $\deg f_E \leq r$.

Now consider the matrix E_2R. We can write

$$E_2R = \left[\ \tilde{E}_2 \ \middle|\ 0\ \right]$$

where $\tilde{E}_2$ is an $(n-k) \times r$ matrix of rank r. Hence

$$XE_2R = \left[\ X\tilde{E}_2 \ \middle|\ 0\ \right].$$

First we prove that the entries of the matrix $X\tilde{E}_2$ are algebraically independent over $\mathbb{F}_q$. Fix $1 \leq i \leq k$ and denote by $(X\tilde{E}_2)_i$ the i-th row of the matrix $X\tilde{E}_2$. Then consider the polynomials $(X\tilde{E}_2)_{ij}$, for $j = 1, \ldots, r$, that only involve the variables $x_{(i-1)(n-k)+1}, \ldots, x_{i(n-k)}$. The Jacobian of these polynomials is $\tilde{E}_2^T$, whose rows are linearly independent over $\mathbb{F}_q$. Therefore the elements in every row are algebraically independent over $\mathbb{F}_q$. Moreover different rows involve different variables, hence we can conclude that the entries of the matrix $X\tilde{E}_2$ are algebraically independent over $\mathbb{F}_q$.

At this point consider the set of all $r \times r$ minors of $X\tilde{E}_2$. These minors are all different and hence linearly independent over $\mathbb{F}_q$, otherwise a non-trivial linear combination of them that gives 0 would produce a non-trivial polynomial relation between the entries of $X\tilde{E}_2R$. Now observe that the degree r term of f_E is a linear combination of these minors. If we write

$$E_1R = \left[\ * \ \middle|\ \tilde{E}_1\ \right],$$

where $\tilde{E}_1 \in \mathbb{F}_q^{k\times(k-r)}$, then the coefficients of this linear combination are given by the $(k-r)\times(k-r)$ minors of $\tilde{E}_1$, multiplied by $\det(R)^{-1}$. Since E^TR has rank k and the last $k - r$ columns of E_2R are 0, it follows that the columns of $\tilde{E}_1$ are linearly independent, and hence at least one of the coefficients of the linear combination is non-zero. This proves that the degree r term of f_E is non-zero, and hence $\deg f_E = r$. □

We can now give the main result of this subsection, an upper bound on the probability that a random generator matrix generates an MRD code:

Theorem 4.6. *Let $X \in \mathbb{F}_{q^m}^{k(n-k)}$ be randomly chosen. Then*

$$\Pr\big(\ \mathrm{rs}[I_k \mid X] \text{ is an MRD code } \big) \geq 1 - \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m}.$$

Proof. For every $r = 0, 1, \ldots, k$ we define the set

$$\mathcal{T}_r = \{E \in \mathcal{T}(k,n) \mid \dim(\mathcal{U}_0 \cap \mathrm{rs}(E)) = k - r\},$$

where

$$\mathcal{U}_0 := \mathrm{rs}[\ I_k \mid 0\ ] = \big\{(u_1, \ldots, u_n) \in \mathbb{F}_q^n \mid u_{k+1} = u_{k+2} = \ldots = u_n = 0\big\}.$$

By Lemma 2.3 we have

$$|\mathcal{T}_r| = \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}.$$

Moreover, by Lemma 4.5, if $E \in \mathcal{T}_r$, then $\deg f_E = r$. Hence, by the definition of $f^*(x_1, \ldots, x_{k(n-k)})$, we have

$$\deg f^* \leq \sum_{E \in \mathcal{T}(k,n)} \deg f_E = \sum_{r=0}^{k} \sum_{E \in \mathcal{T}_r} \deg f_E = \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}.$$

With Lemma 2.16, the statement follows. □

Remember that we know how to construct MRD codes, namely as Gabidulin codes, for any set of parameters. Hence the probability that a randomly chosen generator matrix generates an MRD code is always greater than zero. However, the lower bound of Theorem 4.6 is not always positive. In particular, for

$$m < k(n-k) + \log_q k$$

we get

$$\begin{aligned} &1 - \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m} \\ =&1 - q^{-m} \left(k \begin{bmatrix} n-k \\ k \end{bmatrix}_q q^{k^2} + \sum_{r=1}^{k-1} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} \right) \\ \leq&1 - q^{-m} \left(k q^{k(n-k)} \right) < 0, \end{aligned}$$

i.e., the bound is not tight (and not sensible) in these cases.

Figure 1 depicts the lower bounds of Theorem 4.1 and Theorem 4.6 for small parameters. One can see that the bounds of Theorem 4.6 really is an improvement over the bound of Theorem 4.1.

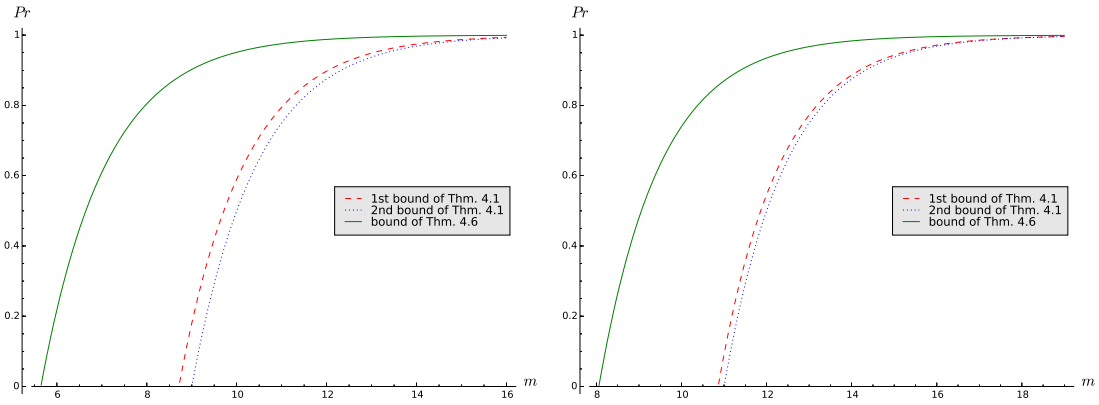

Figure 1: Lower bounds on the probability that a randomly chosen generator matrix in $\mathbb{F}_{2^m}^{2\times 4}$ (left) and $\mathbb{F}_{2^m}^{2\times 5}$ (right) generates an MRD code.

4.2 Probability for Gabidulin codes

We have seen in Theorem 3.4 that the set of matrices in $\mathbb{F}_{q^m}^{k\times n}$ in systematic form that generate a generalized Gabidulin code with parameter s (such that $0 < s < m$ with $\gcd(s, m) = 1$) is in one-to-one correspondence with a subset of the set

$$\left\{ X \in \mathbb{F}_{q^m}^{k\times(n-k)} \mid \operatorname{rk}(X^{(q^s)} - X) = 1 \right\},$$

namely with the elements that represent an MRD code. By Lemma 2.8 we furthermore know that, if X has entries from $\mathbb{F}_q$, then $\operatorname{rs}[\, I_k \mid X \,]$ is not MRD. Hence the set of matrices in systematic form that generate a Gabidulin code is in one-to-one correspondence with a subset of the set

$$\mathcal{G}(s) := \left\{ X \in (\mathbb{F}_{q^m} \setminus \mathbb{F}_q)^{k\times(n-k)} \mid \operatorname{rk}(X^{(q^s)} - X) = 1 \right\}.$$

For simplicity we make the following estimation of the probability that a randomly chosen generator matrix generates a generalized Gabidulin code.

Lemma 4.7. *Let $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$ be randomly chosen. Then*

$$\Pr\big(\operatorname{rs}[I_k \mid X] \text{ is a gen. Gabidulin code}\big) \leq \sum_{\substack{0<s<m \\ \gcd(s,m)=1}} \Pr\big(X \in \mathcal{G}(s)\big) = \sum_{\substack{0<s<m \\ \gcd(s,m)=1}} \frac{|\mathcal{G}(s)|}{q^{mk(n-k)}}.$$

Proof. The inequality follows from the fact that the set of generalized Gabidulin codes is in one-to-one correspondence with a subset of the set

$$\bigcup_{\substack{0<s<m \\ \gcd(s,m)=1}} \mathcal{G}(s).$$

Since $|\mathbb{F}_{q^m}^{k(n-k)}| = q^{mk(n-k)}$, the statement follows. □

For every integer $0 < s < m$ with $\gcd(m, s) = 1$, we now define the map Φ_s given by

$$\begin{aligned} \Phi_s : \mathbb{F}_{q^m}^{k\times(n-k)} &\longrightarrow \mathbb{F}_{q^m}^{k\times(n-k)} \\ X &\longmapsto X^{(q^s)} - X. \end{aligned}$$

Observe that Φ_s is exactly the function that maps every entry X_{ij} of the matrix X to $\varphi_s(X_{ij})$. Moreover we define the sets

$$\begin{aligned} \mathcal{R}_1 &:= \left\{ A \in \mathbb{F}_{q^m}^{k\times(n-k)} \,|\, \mathrm{rk}(A) = 1 \right\}, \\ \mathcal{R}_1^* &:= \left\{ A \in (\mathbb{F}_{q^m}^*)^{k\times(n-k)} \,|\, \mathrm{rk}(A) = 1 \right\}, \\ \mathcal{K} &:= \left(\ker\left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} \right) \right)^{k\times(n-k)}. \end{aligned}$$

We state now the crucial results that will help us to compute an upper bound on the cardinality of the sets $\mathcal{G}(s)$.

Lemma 4.8. *1. Given a matrix $A \in \mathbb{F}_{q^m}^{k\times(n-k)}$, there exists a matrix $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$ such that $\Phi_s(X) = A$ if and only if $A \in \mathcal{K}$.*

2. If $A \in \mathcal{R}_1$, then

$$|\Phi_s^{-1}(A)| = \begin{cases} 0 & \text{if } A \notin \mathcal{K} \\ q^{k(n-k)} & \text{if } A \in \mathcal{K}. \end{cases}$$

3. For every integer s coprime to m

$$\mathcal{G}(s) = \Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}),$$

and

$$|\mathcal{G}(1)| = |\mathcal{G}(s)| = q^{k(n-k)} |\mathcal{R}_1^* \cap \mathcal{K}|.$$

Proof. 1. Since Φ_s is the function that maps every entry X_{ij} of the matrix X to $\varphi_s(X_{ij})$, we have that $A \in \mathrm{Im}(\Phi_s)$ if and only if every entry A_{ij} of A belongs to $\mathrm{Im}(\varphi_s)$. By Lemma 2.2 part 6 this is true if and only if every A_{ij} belongs to $\ker\left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} \right)$.

2. If $A \notin \mathcal{K}$, then by part 1 this means that $\Phi_s^{-1}(A) = \emptyset$. Otherwise, again by part 1, $\Phi_s^{-1}(A) \neq \emptyset$. In this case every entry A_{ij} belongs to $\mathrm{Im}(\varphi_s)$, and since φ_s is linear over $\mathbb{F}_q$, $|\varphi_s^{-1}(A_{ij})| = |\ker(\varphi_s)|$. Since, by Lemma 2.2,

$$|\ker(\varphi_s)| = \frac{|\mathbb{F}_{q^m}|}{|\mathrm{Im}(\varphi_s)|} = q,$$

and A has $k(n-k)$ entries, we get $|\Phi_s^{-1}(A)| = q^{k(n-k)}$.

3. Observe that $\mathcal{R}_1^* = \mathcal{R}_1 \cap \left(\mathbb{F}_{q^m}^*\right)^{k\times(n-k)}$. Moreover

$$\Phi_s^{-1}(\mathcal{R}_1) = \left\{X \in \mathbb{F}_{q^m}^{k\times(n-k)} \mid \mathrm{rk}(X^{(q^s)} - X) = 1\right\}$$

and, by Lemma 2.2 part 5,

$$\Phi_s^{-1}(\left(\mathbb{F}_{q^m}^*\right)^{k\times(n-k)}) = \left(\mathbb{F}_{q^m} \setminus \mathbb{F}_q\right)^{k\times(n-k)}.$$

Hence

$$\Phi_s^{-1}(\mathcal{R}_1^*) = \Phi_s^{-1}(\mathcal{R}_1 \cap \left(\mathbb{F}_{q^m}^*\right)^{k\times(n-k)}) = \Phi_s^{-1}(\mathcal{R}_1) \cap \Phi_s^{-1}(\left(\mathbb{F}_{q^m}^*\right)^{k\times(n-k)}) = \mathcal{G}(s).$$

Now we can write

$$\mathcal{R}_1^* = (\mathcal{R}_1^* \cap \mathcal{K}) \cup (\mathcal{R}_1^* \cap \mathcal{K}^c)$$

and by part 1 we have that $\Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}^c) = \emptyset$. Then

$$\mathcal{G}(s) = \Phi_s^{-1}(\mathcal{R}_1^*) = \Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}) \cup \Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}^c) = \Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K}).$$

By part 2 we have $\left|\Phi_s^{-1}(\mathcal{R}_1^* \cap \mathcal{K})\right| = q^{k(n-k)}|\mathcal{R}_1^* \cap \mathcal{K}|$, which proves the statement. □

In analogy to the previous subsection we now first derive a straight-forward upper bound on the probability that a random generator matrix gives rise to a generalized Gabidulin code. Afterwards we will improve this bound.

Theorem 4.9. *Let $X \in \mathbb{F}_{q^m}^{k(n-k)}$ be randomly chosen. Denote by $\phi(m)$ the Euler-ϕ-function. Then*

$$\Pr\big(\ \mathrm{rs}[I_k \mid X] \text{ is a generalized Gabidulin code }\big) \leq \phi(m)(2q^{1-m})^{\lfloor\frac{k}{2}\rfloor\lfloor\frac{n-k}{2}\rfloor}$$

Proof. We want to derive the cardinality of $\mathcal{G}(s)$ for any valid s. For this, by Lemma 4.8 part 3, we note that these cardinalities are all equal to the cardinality of $\mathcal{G}(1)$. Now for any $X \in (\mathbb{F}_{q^m} \setminus \mathbb{F}_q)^{k\times(n-k)}$ the rank of $X^{(q)} - X$ is greater than zero. Therefore we can also write

$$\mathcal{G}(1) = \left\{X \in (\mathbb{F}_{q^m} \setminus \mathbb{F}_q)^{k\times(n-k)} \mid \mathrm{rk}(X^{(q)} - X) \leq 1\right\}.$$

The condition that $\mathrm{rk}(X^{(q)} - X) \leq 1$ is equivalent to that any 2×2-minor of $X^{(q)} - X$ is zero. Hence a necessary condition is that any set of non-intersecting minors is zero. We have $\lfloor\frac{k}{2}\rfloor\lfloor\frac{n-k}{2}\rfloor$ many such non-intersecting minors, each of which has degree at most $2q$ if we see the entries of X as the variables $x_1, \ldots, x_{k(n-k)}$. With Lemma 2.16 we get for each minor M_{ij},

$$\Pr(M_{ij} = 0) \leq 2q^{1-m}.$$

Since the non-intersecting minors are independent events, the probability that all of these are zero is at most

$$(2q^{1-m})^{\lfloor\frac{k}{2}\rfloor\lfloor\frac{n-k}{2}\rfloor}.$$

With Lemma 4.7 and the fact that the number of s with $\gcd(s, m) = 1$ is given by $\phi(m)$, the statement follows. □

To improve the above bound we need the following lemma.

Lemma 4.10. *The set $\mathcal{R}_1^* \cap \mathcal{K}$ is in one-to-one correspondence with the set*

$$V_R := \left\{ (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{F}_{q^m}^k \times \mathbb{F}_{q^m}^{n-k-1} \mid \alpha_i, \alpha_i\beta_j \in \ker\left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\right) \setminus \{0\} \right\}$$
$$= \left\{ (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{F}_{q^m}^k \times \mathbb{F}_{q^m}^{n-k-1} \mid \alpha_i, \in \ker\left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\right) \setminus \{0\}, \beta_j \in \bigcap_{i=1}^{k} \ker\left(\mathrm{T}_{\alpha_i}\right) \setminus \{0\} \right\}$$

via the map $\psi : V_R \longrightarrow \mathcal{R}_1^* \cap \mathcal{K}$, given by

$$(\boldsymbol{\alpha}, \boldsymbol{\beta}) \longmapsto \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{bmatrix} [1, \beta_1, \ldots, \beta_{n-k-1}],$$

and hence

$$|\mathcal{R}_1^* \cap \mathcal{K}| \leq (q^{m-1} - 1)^{n-1}$$

Proof. From the definition of the set V_R it is clear that the map ψ is well-defined, i.e., it maps every element in V_R to an element in $\mathcal{R}_1^* \cap \mathcal{K}$.

Let $(\boldsymbol{\alpha}, \boldsymbol{\beta})$, $(\boldsymbol{\gamma}, \boldsymbol{\delta})$ be two elements that have the same image. Then the first column of $\psi(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and the first column of $\psi(\boldsymbol{\gamma}, \boldsymbol{\delta})$ are equal, hence $\boldsymbol{\alpha} = \boldsymbol{\gamma}$. Also the first rows of $\psi(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and $\psi(\boldsymbol{\gamma}, \boldsymbol{\delta})$ are equal, thus $\alpha_1\beta_j = \gamma_1\delta_j$ for every $j = 1, \ldots, n-k-1$, and since $\alpha_1 = \gamma_1 \neq 0$ we get $\boldsymbol{\beta} = \boldsymbol{\delta}$ and this shows the injectivity of the map ψ.

In order to show the surjectivity consider a rank 1 matrix $A \in \mathcal{R}_1^* \cap \mathcal{K}$ with entries A_{ij}. Consider the vectors $\boldsymbol{\alpha} = (A_{11}, \ldots, A_{k1})^T$ and

$$\boldsymbol{\beta} = A_{11}^{-1}(A_{12}, \ldots, A_{1(n-k)})^T.$$

It is clear that $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in V_R$, and that $\psi(\boldsymbol{\alpha}, \boldsymbol{\beta}) = A$.

At this point for every α_i we have $q^{m-1} - 1$ possible choices, while for every β_i we have a number of choices that is less or equal to $|\ker(T_{\alpha_1}) \setminus \{0\}|$, that is again $q^{m-1} - 1$. Therefore we get

$$|\mathcal{R}_1^* \cap \mathcal{K}| \leq (q^{m-1} - 1)^{n-1}.$$

□

We can now formulate the main result concerning the probability that a random linear rank-metric code is a generalized Gabidulin code.

Theorem 4.11. *Let $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$ be randomly chosen. Then*

$$\Pr\left(\mathrm{rs}[I_k \mid X] \text{ is a gen. Gabidulin code } \right) \leq \phi(m) q^{-(m-1)(n-k-1)(k-1)},$$

where ϕ denotes the Euler-ϕ function.

Proof. We have already seen in Lemma 4.7 that

$$\Pr\big(\text{ rs}[I_k \,|\, X] \text{ is a gen Gabidulin code }\big) \leq \sum_{\substack{0<s<m \\ (s,m)=1}} \frac{|\mathcal{G}(s)|}{q^{mk(n-k)}}.$$

By Lemma 4.8 part 3, the sets $\mathcal{G}(s)$ all have cardinality $q^{k(n-k)}|\mathcal{R}_1^*|$, thus

$$\sum_{\substack{0<s<m \\ (s,m)=1}} \frac{|\mathcal{G}(s)|}{q^{mk(n-k)}} = \phi(m)\frac{q^{k(n-k)}|\mathcal{R}_1^* \cap \mathcal{K}|}{q^{mk(n-k)}}.$$

Moreover by Lemma 4.10, we know that $|\mathcal{R}_1^* \cap \mathcal{K}| \leq (q^{m-1}-1)^{n-1} \leq q^{(m-1)(n-1)}$. Combining all the inequalities implies the statement. □

We can now give the final main result of this work, that proves the existence of linear MRD codes that are not generalized Gabidulin codes for almost every set of parameters.

Theorem 4.12.

- *For any prime power q, and for any $1 < k < n-1$, there exists an integer $M(q,k,n)$ such that, for every $m \geq M(q,k,n)$, there exists a k-dimensional linear MRD code in $\mathbb{F}_{q^m}^n$ that is not a generalized Gabidulin code.*
- *An integer $M(q,k,n)$ with this property can be found as the minimum integer solution of the inequality*

$$1 - \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m} > (m-1)q^{-(m-1)(n-k-1)(k-1)} \tag{1}$$

  taken over all $m \in \mathbb{N}$.

Proof. For fixed q, k and n consider the function

$$\begin{aligned} F(m) &= \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2} q^{-m} + (m-1)q^{-(m-1)(n-k-1)(k-1)} \\ &= aq^{-m} + (m-1)q^{-c(m-1)}, \end{aligned}$$

where

$$a := \sum_{r=0}^{k} r \begin{bmatrix} k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-k \\ r \end{bmatrix}_q q^{r^2}, \quad c := (n-k-1)(k-1).$$

Since $k \neq 1, n-1$, we have $c > 0$. In this case $F(m)$ is the sum of two non-increasing functions and hence it is non-increasing. Therefore the function $1 - F(m)$ is non-decreasing. Moreover it is easy to see that

$$\lim_{m \to +\infty} 1 - F(m) = 1.$$

This means that the set of the solutions of Inequality (1) is non-empty. Then it has a minimum solution $M(q,k,n)$. Since the function $1-F(m)$ is non-decreasing, every $m \geq M(q,k,n)$ is also a solution of (1). Hence, by Theorems 4.6 and 4.11, we have the following chain of inequalities for every $m \geq M(q,k,n)$,

$$\Pr\big(\mathrm{rs}[I_k \,|\, X] \text{ is MRD}\big) \geq 1 - aq^{-m} > (m-1)q^{-c(m-1)} \geq \Pr\big(\mathrm{rs}[I_k \,|\, X] \text{ is gen. Gabidulin}\big),$$

which concludes the proof. □

In Figures 2 and Figures 3 we compare the bounds derived in this section with experimental results, which we got by randomly generating over 500 rank-metric codes. The continuous lines show the bounds, the dotted lines show the experimental probabilities. In Figure 2 we see that Gabidulin codes are very few among all MRD codes when the extension degree m is large. The probabilities for generalized Gabidulin codes decrease so quickly for increasing parameters that we show them separately, in logarithmic scale, in Figure 3. Notice that from $m = 10$ it is very difficult to generate a generalized Gabidulin code randomly and thus, experimentally we got a probability zero. This is why the experimental result was shown only up to $m = 9$.

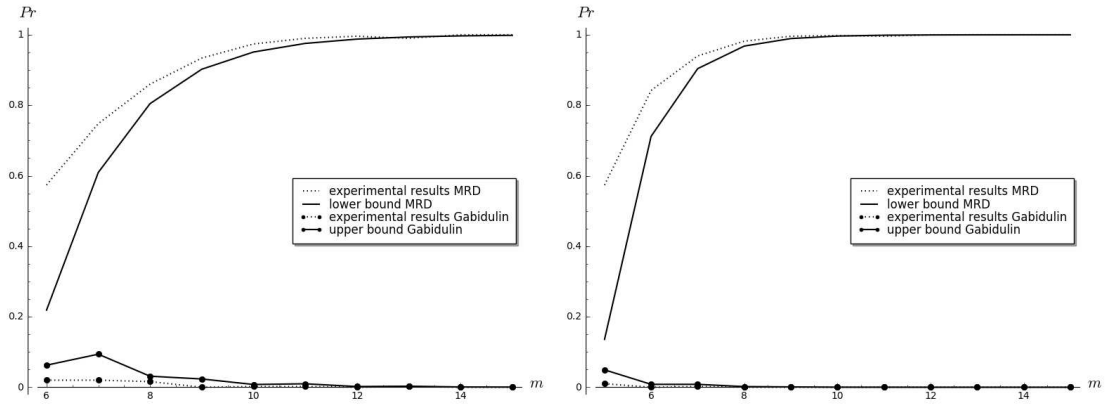

Figure 2: Bounds and experimental results for MRD and generalized Gabidulin codes in $\mathbb{F}_{2^m}^{2\times 4}$ and $\mathbb{F}_{3^m}^{2\times 4}$.

5 Conclusion

In this work we have shown that, over the algebraic closure of a given finite field, MRD codes and non-Gabidulin codes are generic sets among all linear rank-metric codes. For this we have used two known criteria for these two properties, which give rise to algebraic descriptions of the respective sets. Afterwards we have used the same two criteria to establish a lower bound on the probability that a randomly chosen systematic generator matrix generates an MRD code, and an upper bound on the probability that a randomly

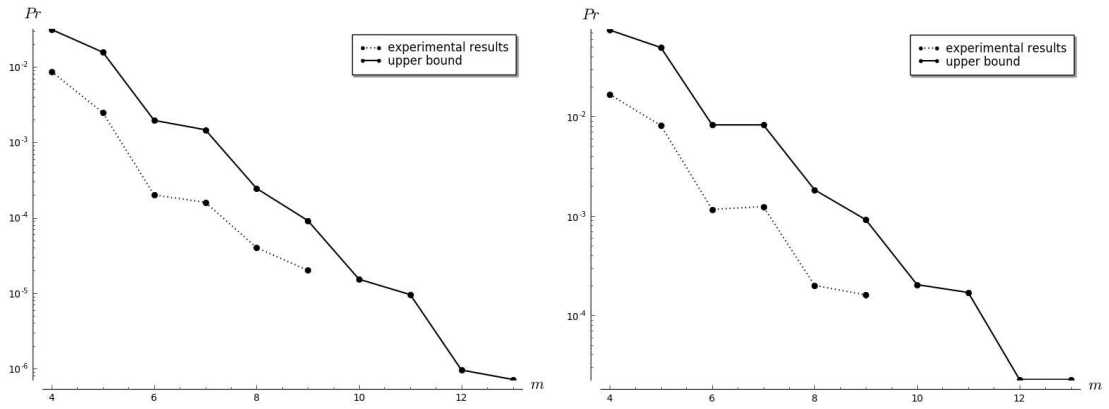

Figure 3: Bounds and experimental results for generalized Gabidulin codes in $\mathbb{F}_{2^m}^{2\times 5}$ and $\mathbb{F}_{3^m}^{2\times 4}$.

chosen systematic generator matrix generates a generalized Gabidulin code. With these two bounds we were then able to show that non-Gabidulin MRD codes exists for any length n and dimension $1 < k < n-1$, as long as the underlying field size is large enough.

References

[1] Berger, T.P.: Isometries for rank distance and permutation group of Gabidulin codes. IEEE Transactions on Information Theory **49**(11), 3016 – 3019 (2003). DOI 10.1109/TIT.2003.819322

[2] Cossidente, A., Marino, G., Pavese, F.: Non-linear maximum rank distance codes. preprint (2015)

[3] de la Cruz, J., Kiermaier, M., Wassermann, A., Willems, W.: Algebraic structures of MRD codes. arXiv:1502.02711 **[cs.IT]** (2015). URL `http://arxiv.org/abs/1502.02711`

[4] Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. Journal of Combinatorial Theory, Series A **25**(3), 226–241 (1978). DOI 10.1016/0097-3165(78)90015-8. URL `http://dx.doi.org/10.1016/0097-3165(78)90015-8`

[5] Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy Peredachi Informatsii **21**(1), 3–16 (1985)

[6] Horlemann-Trautmann, A., Marshall, K.: New criteria for MRD and Gabidulin codes and some rank-metric code constructions. arXiv:1507.08641 **[cs.IT]** (2015)

[7] Kshevetskiy, A., Gabidulin, E.: The new construction of rank codes. In: Proceedings of the International Symposium on Information Theory (ISIT) 2005, pp. 2105–2108 (2005). DOI 10.1109/ISIT.2005.1523717

[8] Lidl, R., Niederreiter, H.: Introduction to Finite Fields and their Applications. Cambridge University Press, Cambridge, London (1994). Revised edition

[9] Morrison, K.: Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes. IEEE Transactions on Information Theory **60**(11), 7035–7046 (2014). DOI 10.1109/TIT.2014.2359198

[10] Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomial identities. J. ACM **27**(4), 701–717 (1980)

[11] Sheekey, J.: A new family of linear maximum rank distance codes. arXiv:1504.01581 [cs.IT] (2015)

[12] Wan, Z.X.: Geometry of matrices. World Scientific, Singapore (1996). In memory of Professor L.K. Hua (1910 – 1985)